

# BEC AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-016037

(43)Date of publication of application : 17.01.2003

(51)Int.Cl.

G06F 15/00

H04L 9/32

(21)Application number : 2001-198141

(71)Applicant : NIFTY CORP

(22)Date of filing : 29.06.2001

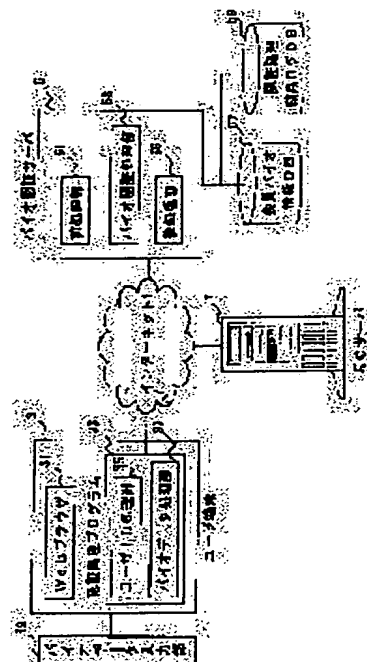
(72)Inventor : TAWARA TADAYUKI

### (54) METHOD FOR AUTHENTICATION PROCESSING

(57)Abstract:

**PROBLEM TO BE SOLVED:** To safely perform biometric authentication processing at a user terminal in a system comprising a center server and a user terminal.

**SOLUTION:** User information is acquired according to a request from an EC(electronic commerce) server 7 to be transmitted to a bio authentication server 5, an input of biometric data from a user is prompted. When receiving the registered data from the server 5, the processing is performed by using the inputted data by the user and the received registered data to transmit a result of the processing to the server 7. When receiving a request for the biometric data from the server 5, the biometric data inputted from the user is transmitted to the server 5.



### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2003-16037

(P 2003-16037A)

(43) 公開日 平成15年1月17日 (2003. 1. 17)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	ターム (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 B	5B085
			3 3 0 F 5J104
H 0 4 L 9/32		H 0 4 L 9/00 6 7 3 D	

審査請求 未請求 請求項の数 10 OL

(全 12 頁)

(21) 出願番号 特願2001-198141 (P2001-198141)

(22) 出願日 平成13年6月29日 (2001. 6. 29)

(71) 出願人 591117192

ニフティ株式会社

東京都品川区南大井6-26-1

(72) 発明者 田原 忠行

東京都品川区南大井六丁目26番1号 ニフティ株式会社内

(74) 代理人 100103528

弁理士 原田 一男

F ターム (参考) 5B085 AE02 AE04 AE09 AE23 AE25

5J104 AA07 KA01 KA16 KA17 KA18

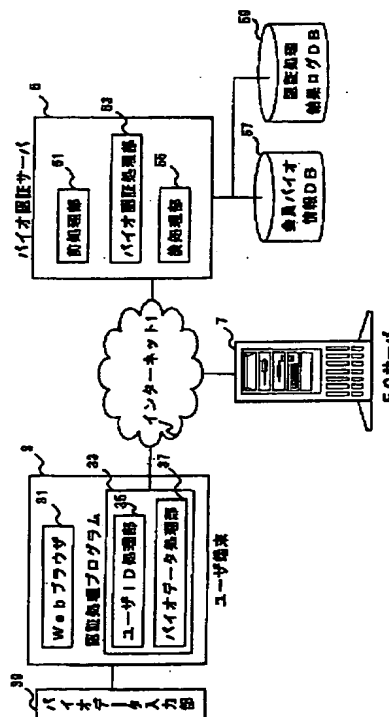
MA04 PA07 PA10

## (54) 【発明の名称】 認証処理方法

## (57) 【要約】

【課題】 センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイOMETRICS認証処理を安全に実施する。

【解決手段】 ECサーバ7からの要求に応じて、ユーザ識別情報を取得してバイオ認証サーバ5に送信する。また、ユーザに対してバイOMETRICS・データの入力を促す。倍認証サーバ5から登録バイOMETRICS・データを受信すると、ユーザにより入力されたバイOMETRICS・データとバイオ認証サーバ5から受信した登録バイOMETRICS・データとを用いて、バイOMETRICS認証処理を実施する。そして、バイOMETRICS認証処理の結果を、ECサーバ7に送信する。また、バイOMETRICS認証処理の結果を、バイオ認証サーバ5に送信し、バイオ認証サーバ5からバイOMETRICS・データの要求を受信した場合には、ユーザにより入力されたバイOMETRICS・データをバイオ認証サーバ5に送信する。



# 【特許請求の範囲】

【請求項 1】 認証結果要求元コンピュータからの要求に応じて、ユーザ識別情報を取得してセンタ・サーバに送信するユーザ識別情報送信ステップと、ユーザに対してバイオメトリクス・データの入力を促すステップと、前記センタ・サーバから登録バイオメトリクス・データを受信するステップと、前記ユーザにより入力されたバイオメトリクス・データと前記センタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施するステップと、前記バイオメトリクス認証処理の結果を、前記認証結果要求元コンピュータに送信するステップと、を含む認証処理方法。

【請求項 2】 前記バイオメトリクス認証処理の結果を、前記センタ・サーバに送信するステップと、前記センタ・サーバからバイオメトリクス・データの要求を受信した場合には、前記バイオメトリクス認証処理において用いられたバイオメトリクス・データを前記センタ・サーバに送信するステップと、をさらに含む請求項 1 記載の認証処理方法。

【請求項 3】 前記センタ・サーバから前記登録バイオメトリクス・データの代わりにバイオメトリクス・データ送信要求を受信した場合には、前記ユーザの入力にかかるバイオメトリクス・データを前記センタ・サーバに送信するステップをさらに含む請求項 1 又は 2 記載の認証処理方法。

【請求項 4】 前記ユーザ識別情報送信ステップが、ユーザ機器の固有情報、又は前記ユーザにより予め入力された識別情報のいずれかを前記ユーザ識別情報として取得して前記センタ・サーバに送信するステップを含む請求項 1 乃至 3 のいずれか 1 つ記載の認証処理方法。

【請求項 5】 ユーザ端末からユーザ識別情報を受信するステップと、前記ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報 DB から取り出し、前記ユーザ端末に送信するステップと、前記ユーザ端末から前記登録バイオメトリクス情報に基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、前記登録バイオメトリクス・データの更新をすべきか判断するステップと、更新すべきと判断された場合には、前記ユーザ端末にバイオメトリクス・データ要求を送信するステップと、を含む認証処理方法。

【請求項 6】 ユーザ端末からユーザ識別情報を受信するステップと、ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定するステップと、

前記ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、前記ユーザ識別情報に対応する登録バイオメトリクス・データを取得して前記ユーザ端末に送信するステップと、前記センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求を前記ユーザ端末に送信するステップと、を含む認証処理方法。

【請求項 7】 請求項 1 乃至 6 のいずれか 1 つに記載された認証処理方法をコンピュータに実行させるためのコンピュータ・プログラム。

【請求項 8】 認証結果要求元コンピュータからの要求に応じて、ユーザ識別情報を取得してセンタ・サーバに送信する手段と、ユーザに対してバイオメトリクス・データの入力を促す手段と、前記センタ・サーバから登録バイオメトリクス・データを受信する手段と、前記ユーザにより入力されたバイオメトリクス・データと前記センタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施する手段と、前記バイオメトリクス認証処理の結果を、前記認証結果要求元コンピュータに送信する手段と、を有するコンピュータ。

【請求項 9】 ユーザ端末からユーザ識別情報を受信する手段と、前記ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報 DB から取り出し、前記ユーザ端末に送信する手段と、前記ユーザ端末から前記登録バイオメトリクス・データに基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、前記登録バイオメトリクス・データの更新をすべきか判断する手段と、更新すべきと判断された場合には、前記ユーザ端末にバイオメトリクス・データ要求を送信する手段と、を有するコンピュータ・システム。

【請求項 10】 ユーザ端末からユーザ識別情報を受信する手段と、ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定する手段と、前記ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、前記ユーザ識別情報に対応する登録バイオメトリクス・データを取得して前記ユーザ端末に送信する手段と、前記センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求を前記ユーザ端末に送信する手段と、を有するコンピュータ・システム。

**【発明の詳細な説明】****【0001】**

**【発明が属する技術分野】** 本発明は、バイオメトリクス認証処理技術に関する。

**【0002】**

**【従来の技術】** 従来、ネットワークを介したバイオメトリクス認証処理は、ユーザ端末から認証サーバにバイオメトリクス・データ（以下、バイオ・データとも呼ぶ）を送信し、当該認証サーバにおいてバイオ・データを用いた認証処理を実施していた。また、認証サーバに登録されたバイオ・データは、ユーザが希望したときのみ登録変更が行われる構成であった。

**【0003】**

**【発明が解決しようとする課題】** 従来技術によれば、バイオ・データはデータ・サイズが大きく、且つ認証サーバでの解析には比較的大きな処理能力が必要とされる。また、バイオ・データのユーザ端末から認証サーバへの送信は、通信回線品質や音量などにより認証サーバで解析が可能となるレベルになるまで何回も要求される場合もあり、通信回線網や認証サーバの負担が大きかった。従って、多くのユーザが認証サーバに一度にアクセスすると、処理時間が長くなったり、クラッカーによる大量の不正データ送付（いわゆるD o S攻撃（Denied of Service attack）によるサーバ麻痺の危険性があった。

**【0004】** これらの問題は主に認証サーバにおいてバイオメトリクス認証処理を実施するための生ずるものである。

**【0005】** 従って、本発明の目的は、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を実施するための技術を提供することである。

**【0006】** 他の目的は、センタ・サーバにおいて必要な時に登録されたバイオメトリクス・データの更新を要求を行うことができるようにするための技術を提供することである。

**【0007】** さらに他の目的は、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を安全に実施するための技術を提供することである。

**【0008】**

**【課題を解決するための手段】** 本発明の第1の態様に係る、ユーザ端末（例えば実施の形態におけるユーザ端末3）における認証処理方法は、認証結果要求元コンピュータ（例えば実施の形態におけるECサーバ7）からの要求に応じて、ユーザ識別情報を取得してセンタ・サーバ（例えば実施の形態におけるバイオ認証サーバ5）に送信するユーザ識別情報送信ステップと、ユーザに対してバイオメトリクス・データの入力を促すステップと、センタ・サーバから登録バイオメトリクス・データを受信するステップと、ユーザにより入力されたバイオメ

トリクス・データとセンタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施するステップと、バイオメトリクス認証処理の結果を、認証結果要求元コンピュータに送信するステップとを含む。

**【0009】** このようにすれば、センタ・サーバの処理負荷は大幅に減少でき、クラッカー等によるD o S攻撃に対処しやすくなる。また、バイオメトリクス・データについては、一度だけネットワークを介して送信されるだけであるから、ネットワークの負荷も下げることができる。さらに、ADSL（Asymmetric Digital Subscriber Line）をユーザが用いている場合には、サイズの大きいバイオメトリクス・データのダウンロードも高速に行うことができる。なお、バイオメトリクス認証には、ユーザの顔による顔認証、音声認証、指紋認証、サイン認証などが含まれる。

**【0010】** また、本発明の第1の態様において、バイオメトリクス認証処理の結果を、センタ・サーバに送信するステップと、センタ・サーバからバイオメトリクス・データの要求を受信した場合には、バイオメトリクス認証処理において用いられたバイオメトリクス・データをセンタ・サーバに送信するステップとをさらに含むような構成であってもよい。

**【0011】** これにより、センタ・サーバにおいては、ユーザのバイオメトリクス・データの経年変化に対応して登録バイオメトリクス・データの更新を行うことができるようになる。

**【0012】** さらに、本発明の第1の態様において、センタ・サーバから登録バイオメトリクス・データの代わりにバイオメトリクス・データ送信要求を受信した場合には、ユーザの入力にかかるバイオメトリクス・データをセンタ・サーバに送信するステップをさらに含むような構成であってもよい。常にユーザ端末においてバイオメトリクス認証処理を実施するとすると、悪意を持ったユーザが不正な行為を行うこともあるので、例えばランダムに、又はセンタ・サーバの処理負荷状態等に応じて、センタ・サーバにおけるバイオメトリクス認証を実施するようにすれば、不正を防止することができるようになる。

**【0013】** さらに、上で述べたユーザ識別情報送信ステップが、ユーザ機器の固有情報（例えばMACアドレス、CPUのシリアル番号など）、又はユーザにより予め入力された識別情報のいずれかをユーザ識別情報として取得してセンタ・サーバに送信するステップを含むような構成であってもよい。例えば、会員ID以外の識別情報、特にユーザ機器の固有情報等であれば、不正取得の可能性が低くなり、安全な認証処理が行われることとなる。

**【0014】** 本発明の第2の態様に係る、センタ・サーバにおける認証処理方法は、ユーザ端末からユーザ識別

情報を受信するステップと、ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報DBから取り出し、ユーザ端末に送信するステップと、ユーザ端末から登録バイオメトリクス・データに基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、登録バイオメトリクス・データの更新をすべきか判断するステップと、更新すべきと判断された場合には、ユーザ端末にバイオメトリクス・データ要求を送信するステップとを含む。

【0015】このようにすればセンタ・サーバは、登録バイオメトリクス・データを適切な時期に更新することができるようになる。

【0016】本発明の第3の態様に係る、センタ・サーバにおける認証処理方法は、ユーザ端末からユーザ識別情報を受信するステップと、ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定するステップと、ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、ユーザ識別情報に対応する登録バイオメトリクス・データを取得してユーザ端末に送信するステップと、センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求をユーザ端末に送信するステップとを含む。このような構成によりユーザの不正行為の抑止効果を期待することができるようになる。

【0017】また、本発明の第1乃至3の態様に係る方法をコンピュータに実行させるためのプログラムを作成することも可能であって、当該プログラムは、例えばフレキシブル・ディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。なお、ネットワークを介して配布される場合もある。また、処理途中のデータについては、コンピュータのメモリに一時保管される。

#### 【0018】

【発明の実施の形態】本発明の一実施の形態に係るシステム概要を図1に示す。コンピュータ・ネットワークであるインターネット1には、1又は複数のユーザ端末3と、バイオ認証サーバ5と、1又は複数のEC (Electronic Commerce) サーバ7とが接続されている。

【0019】ユーザ端末3には、例えばウェブ (Web) ブラウザ31がインストールされており、Webサーバ機能を有するECサーバ7との間でHTTP (Hypertext Transfer Protocol) に従って通信を行い、受信したWebページ・データ (例えばHTML (Hypertext Markup Language) ファイルや参照されている場合には画像ファイルを含む) を表示装置に表示する。また、ユーザ端末3には、本実施の形態において主な処理を実施する認証処理プログラム33もインストールされている。この認証処理プログラム33は、例えばWebブラ

ウザ31のプラグイン (Plug-in) プログラムとして会員 (登録ユーザ) に配布されるような場合もあれば、Webブラウザ31と連携する別のプログラムとして会員 (登録ユーザ) に配布されるような場合もある。

【0020】認証処理プログラム33には、会員IDやその他のユーザ識別情報を処理するユーザID処理部35と、ユーザにバイオ・データの入力を行わせるための処理、当該バイオ・データとバイオ認証サーバ5から受信した登録バイオ・データを用いた認証処理、バイオ認証サーバ5からの要求に応じて入力バイオ・データをバイオ認証サーバ5に送信する処理等を実施するバイオデータ処理部37とが含まれる。

【0021】ユーザ端末3には、バイオデータ入力部39が接続されている。例えば顔認証の場合、このバイオデータ入力部39は顔の画像データを取得するためのカメラである。また、音声認証の場合には、音声を電気信号に変換するマイクロフォンである。指紋認証の場合には、指紋読取装置である。サイン認証の場合には、手書き文字の入力を行うためのデジタイザ等の座標入力装置である。その他のバイオメトリクス認証処理の場合には、それに対応する入力装置である。これらの装置については従来と同じであるから、これ以上説明しない。

【0022】ECサーバ7は、Webサーバ機能を有する電子商取引を行うためのサーバである。多くの店舗が出店されている電子モールであってもよいし、一つの店舗のためのだけのECサーバであってもよい。ECサーバ7の構成は、バイオ認証処理に関係する、ユーザ端末3及びバイオ認証サーバ5とのインターフェースの部分のみが従来と異なる部分である。これについては、以下で説明する処理フローにて明らかにする。

【0023】バイオ認証サーバ5には、前処理部51と、バイオメトリクス認証処理を実施するバイオ認証処理部53と、後処理部55とが含まれる。各処理部の処理内容については後に説明する。また、バイオ認証サーバ5は、会員IDを含む会員の個人情報と、バイオ・データとを格納する会員バイオ情報データベース (DB) 57と、認証処理結果ログDB59とを管理している。なお、ユーザは、予め何らかの方法にてバイオ認証サーバ5に会員の個人情報とバイオ・データとの登録を行っておく必要がある。例えば、会員登録用のWebサーバ及びユーザ端末3を用いて又は申込書を用いて会員登録の申し込みを行い、バイオ・データを電話や店舗における直接の登録や郵送による登録を行う。

【0024】次に図2乃至図5を用いて図1に示されたシステムの処理フローを説明する。ユーザは、ECサーバ7の例えばショッピングカートのWebページに設けられた購入ボタン等をクリックする。また、ログインが必要なページへのリンクをクリックするような場合もある。そうすると、ユーザ端末3は、ECサーバ7の認証処理が必要となるWebページへアクセスする (ステッ

ブS1)。ECサーバ7は、このアクセスにตอบสนองしてバイオ認証サーバ5へのID送信要求を、ユーザ端末3に送信する(ステップS3)。この際、後に本実施の形態に従って認証処理が行われたことを確認するための第1キーを生成して、ユーザ端末3及びバイオ認証サーバ5に送信する場合もある。ユーザ端末3及びバイオ認証サーバ5は、第1キーを受信し、記憶装置に格納しておく。

【0025】ユーザ端末3は、ID送信要求をECサーバ7から受信すると(ステップS5)、認証処理プログラム33を起動する。認証処理プログラム33のユーザID処理部35は、IDの自動送信が指定済みであるか確認する(ステップS7)。もし、IDの自動送信が指定されていない場合にはステップS19に移行する。一方、IDの自動送信が指定されている場合には、送信すべきIDが会員IDであるか否かを判断する(ステップS9)。もし、会員IDである場合にはステップS17に移行する。会員IDではない場合には、ユーザ端末固有の情報の自動取得が指定されているか否かを判断する(ステップS11)。ユーザ端末固有の情報とは、例えばMAC(Media Access Control)アドレスやCPUのシリアル番号等である。例えば認証処理プログラム33をインストール時等に、これらの情報の使用をユーザが許可し、且つ例えばインターネット1等を経由してバイオ認証サーバ5に予め登録しているものとする。すなわち、会員バイオ情報DB57には、会員IDと機器固有情報との対応関係が記録されている。

【0026】もし、ユーザ端末固有情報の自動取得が指定されていれば、認証処理プログラム33は、ユーザ端末3のユーザ端末固有情報(IDとも呼ぶ)を自動で取得する(ステップS13)。一方、ユーザ端末固有情報の自動取得が指定されていない場合には、認証処理プログラム33のインストール時に入力された固有情報(IDとも呼ぶ)を取得する(ステップS15)。この固有情報は、例えば認証処理プログラム33がインストール時にユーザにより指定された情報である。ユーザ端末固有情報そのものであっても良いし、ユーザにより変更等された情報であってもよい。ステップS13及びステップS15の後にステップS21に移行する。

【0027】ステップS9で送信すべきIDは会員IDであると判断された場合には、認証処理プログラム33のインストール時に入力された会員IDを取得する(ステップS17)。そして、ステップS21に移行する。ステップS7でIDの自動送信が指定されていない場合には、会員IDの入力を促し、ユーザが入力した会員IDを取得する(ステップS19)。

【0028】このようにステップS13、ステップS15、ステップS17、又はステップS19において取得されたIDを、認証処理プログラム33は、暗号化して、バイオ認証サーバ5に送信する(ステップS2

1)。バイオ認証サーバ5の前処理部51は、ユーザ端末3から暗号化されたIDを受信する(ステップS23)。このユーザ端末3の認証処理プログラム33とバイオ認証サーバ5との通信は、専用のプロトコルを用いるようにしても良い。この場合には、悪意のあるユーザによるなりすまし等の攻撃を受けにくくなる。なお、キーを用いてなりすまし等を防止する場合には、認証処理プログラム33は、ECサーバ7により付与された第1キーをIDと共に隠しパラメータとして送信する。この場合、バイオ認証サーバ5は、第1キーを受信すると、ECサーバ7から受信された第1キーと照合する。もし、ユーザ端末3から受信した第1キーと例えば所定時間内にECサーバ7から受信された第1キーとのマッチングが取れない場合には、当該受信したIDを無視する、又は無効としてユーザ端末3に通知する。

【0029】端子A、端子B及び端子Cを介して図3に移行する。

【0030】前処理部51は、暗号化されたIDを復号化し(ステップS25)、バイオ認証サーバ5で認証処理を実施するか否かを判断する(ステップS27)。もし、バイオ認証サーバ5で認証処理を実施する場合には、端子Eを介して図5に移行する。バイオ認証サーバ5で認証処理を実施するか否かは、様々な要素で決定され得る。例えば、ランダムであってもよい。また、バイオ認証サーバ5の処理負荷レベルで決定しても良い。例えば、処理負荷レベルが高い場合にはユーザ端末3において認証処理を実施し、低い場合にはバイオ認証サーバ5で処理するような場合もある。さらに、同一ユーザにつき所定回数ごとにバイオ認証サーバ5で実施するようにしても良い。また、特定のユーザについては常にバイオ認証サーバ5、逆に特定のユーザについては常にユーザ端末3でバイオ認証処理を実施するようにしても良い。さらに、ECサーバ7から指定を受けるような構成であってもよい。例えば、値段が高い場合や特定の商品の場合にはECサーバ7からバイオ認証サーバ5における認証処理を要求するような構成であってもよい。

【0031】もし、ユーザ端末3における認証処理を実施すると判断された場合には、前処理部51は、受信したIDに対応する登録バイオ・データを会員バイオ情報DB57から読み出し(ステップS29)、当該登録バイオ・データを暗号化して、当該暗号化登録バイオ・データをユーザ端末3に送信する(ステップS31)。登録バイオ・データは、ユーザ端末3にインストールされた認証処理プログラム33のバイオデータ処理部37において行われる認証処理において使用しやすい形式に変形されたデータ(例えばモデル・データや特徴データ)である場合もある。なお、キーを用いた処理系である場合には、ここで第2キーを生成してユーザ端末3に暗号化登録バイオ・データと共に送信する場合もある。また、第1及び第2のキーをECサーバ7に送信しておく

場合もある。これによりECサーバ7は、注文情報やECサイトにおけるユーザの識別情報等と第1及び第2キーの対応付けができるようになる。ユーザ端末3及びECサーバ7は、キーを受信し、記憶装置に格納する。

【0032】一方、ユーザ端末3では、バイオデータ処理部37が、ユーザに対してバイオ・データの入力要求する(ステップS33)。これに対してユーザは、バイオデータ入力部39に対してバイオ・データを入力し、バイオデータ処理部37が当該バイオ・データを取得する(ステップS35)。そして、バイオデータ処理部37は、バイオ認証サーバ5から暗号化登録バイオ・データを受信する(ステップS37)。また、バイオデータ処理部37は、暗号化登録バイオ・データを復号化し、登録バイオ・データを復元する(ステップS39)。そして、登録バイオ・データと入力バイオ・データとを用いて認証処理を実施する(ステップS41)。この認証処理については、バイオ・データの種類により異なり且つ基本的に従来と同じであるからここでは説明を省略する。

【0033】そしてバイオデータ処理部37は、認証が成功したか判断する(ステップS43)。もし認証に失敗したと判断された場合には、端子Fを介して図4に移行する。一方、認証に成功したと判断された場合には、認証成功をECサーバ7及びバイオ認証サーバ5に送信する(ステップS45)。もしキーを用いた処理系の場合には、第2キーを隠しパラメータとしてECサーバ7及びバイオ認証サーバ5に送信する。ECサーバ7は、第2キーをユーザ端末3から受信するとバイオ認証サーバ5から受信した第2キーと照合して、正規の処理フロー(特にステップS31)を経て認証成功が通知されているかを確認する。もし、ECサーバ7はバイオ認証サーバ5から同一の第2キーを受信していない場合には認証成功としては取り扱わない場合もある。バイオ認証サーバ5についても同様である。

【0034】ECサーバ7は、ユーザ端末3から認証成功の情報を受信し(ステップS47)、認証後の処理を実施する(ステップS49)。認証後の処理とは、例えば申込受け付け通知を送信したり、決済ページを送信したり、実際に決済処理を実行したりする処理である。但し、これに限定されるものではない。

【0035】バイオ認証サーバ5の前処理部51は、ユーザ端末3から認証成功の情報を受信し(ステップS51)、認証日時を認証処理結果ログDB59に登録する(ステップS53)。例えば、認証成功の情報にECサーバ7についての情報が含まれる場合には、当該情報も認証処理結果ログDB59に格納しても良い。次に、後処理部55は、登録バイオ・データの更新時期になったか否かを判断する(ステップS55)。例えば、所定周期ごとに登録バイオ・データを更新することになっている場合には、当該所定周期を経過したか否かを更新記録

などを参照して判断する。

【0036】もし、登録バイオ・データの更新時期ではないと判断された場合には、処理を終了する。一方、登録バイオ・データの更新時期であると判断された場合には、後処理部55はユーザ端末3にバイオデータ要求を送信する(ステップS57)。ユーザ端末3のバイオデータ処理部37は、バイオデータ要求を受信し(ステップS59)、ステップS35で取得したバイオ・データ又はステップS41における認証処理において処理されたバイオ・データのいずれかを暗号化し、バイオ認証サーバ5に送信する(ステップS61)。バイオ認証サーバ5の後処理部55は、ユーザ端末3から暗号化バイオ・データを受信し、復号化して、会員バイオ情報DB57に登録する(ステップS63)。なお、受信したバイオ・データにさらに処理を施した後に登録することもある。例えば、モデル・データや特徴データを抽出する処理である。さらに、なりすまし等を防止するために、バイオ認証処理部53で認証処理を実施し、認証成功を確認した上で登録するようにしてもよい。

【0037】次に、ステップS43において認証失敗と判断された場合(端子F経由)の処理を図4を用いて説明する。認証失敗の場合には、バイオデータ処理部37は認証処理回数は許容限度内(例えば3回)であるか判断する(ステップS65)。もし、認証処理回数が許容限度内であれば、端子Dを介して図3のステップS33に戻り、ユーザによるバイオ・データの入力を再度求め、再度入力されたバイオ・データを用いて認証処理を実施する。一方、認証処理回数が許容限度を超えていれば、認証失敗をECサーバ7及びバイオ認証サーバ5に送信する(ステップS67)。もし、キーを用いた処理系の場合には、このときに隠しパラメータとして第2キーを合わせて送信する。

【0038】ECサーバ7は、ユーザ端末3から認証失敗を受信すると(ステップS69)、認証要求を無効として取り扱う(ステップS71)。すなわち、発注受付を送信しないようにしたり、決済を実行したりせず、今回は受け付けられない旨の通知を行ったりする。また、バイオ認証サーバ5の前処理部51は、認証失敗の情報を受信し(ステップS73)、当該認証失敗を認証処理結果ログDB59に登録する(ステップS75)。これで処理を終了する。

【0039】これによりユーザ端末3における認証処理が安全に行われる。またネットワークの負荷を軽減でき、且つバイオ認証サーバ5の処理負荷を減らすことができるようになる。さらに、バイオ認証サーバ5における処理負荷を減らすことができるので、DoS攻撃などの対処がしやすくなる。また、ユーザ端末3にインストールされる専用の認証処理プログラム33を用いるためにハッキング等を受けることが少なくなる。さらに、バイオ認証サーバ5の会員バイオ情報DB57に登録され



るバイオ・データを時々更新することにより、バイオ・データの経年変化に対応できるようになる。

【0040】次に図5を用いて図3のステップS27でバイオ認証サーバ5で認証処理を実施すると判断された場合（端子E経由）の処理を説明する。前処理部51がバイオ認証サーバ5で認証処理を実施すると判断すると、バイオ・データの送信要求をユーザ端末3に送信する（ステップS81）。もし、キーを用いる処理系の場合には、第2キーを生成して、ユーザ端末3に第2キーを隠しパラメータとして送信する。ユーザ端末3は第2キーを受信し、記憶装置に格納する。また、第1及び第2キーをECサーバ7に送信する。ECサーバ7は第1及び第2キーを受信し、記憶装置に格納する。

【0041】ユーザ端末3のバイオデータ処理部は、バイオ認証サーバ5からバイオ・データの送信要求を受信し（ステップS83）、ユーザによりバイオデータ入力部39から入力されたバイオ・データ又はバイオ認証サーバ5における認証処理に適した形式に変形したバイオ・データを暗号化し、バイオ認証サーバ5に送信する（ステップS85）。もし、キーを用いる処理系の場合には、第2キーを隠しパラメータとしてバイオ認証サーバ5に送信する。第2キーを受信したバイオ認証サーバ5のバイオ認証処理部53は、第2キーの照合を行って、適正なユーザ端末3から暗号化入力バイオ・データを受信したことを確認する。

【0042】バイオ認証サーバ5のバイオ認証処理部53は、ステップS81の後にIDに対応する登録バイオ・データを会員バイオ情報DB57から読み出す（ステップS87）。また、ユーザ端末3から暗号化入力バイオ・データを受信し、復号化処理を実施する（ステップS89）。そして、バイオ認証処理部53は、登録バイオ・データと入力バイオ・データを用いて認証処理を実施する（ステップS91）。この認証処理については、バイオ・データの種類により異なり且つ基本的に従来と同じであるからここでは説明を省略する。

【0043】そして、バイオ認証処理部53は認証処理の結果が成功を示しているか判断する（ステップS93）。もし、失敗を示している場合にはステップS109に移行する。一方、認証処理の結果が成功を示している場合には、認証成功をユーザ端末3及びECサーバ7に送信する（ステップS95）。ECサーバ7は、バイオ認証サーバ5から認証成功の情報を受信すると（ステップS97）、認証後の処理、例えば発注受付通知の処理や、決済ページの情報をユーザ端末3へ送信する処理、又は決済処理自体を実施する（ステップS99）。また、ユーザ端末3は、バイオ認証サーバ5から認証成功の情報を受信する（ステップS101）。もし、キーを用いた処理系の場合には、バイオ認証サーバ5のバイオ認証処理部53はECサーバ7に隠しパラメータとして第2キーを送信する。ECサーバ7は第2キーを受信

し、以前受信した第2キーと照合することにより、所定の処理フローを経て認証結果が通知されたことを確認することができるようになる。

【0044】バイオ認証サーバ5のバイオ認証処理部53は、認証日時を認証処理結果ログDB59に登録する（ステップS103）。例えば、ECサーバ7についての情報も認証処理結果ログDB59に格納しても良い。次に、後処理部55は、登録バイオ・データの更新時期になったか否かを判断する（ステップS105）。例えば、所定期間ごとに登録バイオ・データを更新することになっている場合には、当該所定期間を経過したか否かを更新記録などを参照して判断する。

【0045】もし、登録バイオ・データの更新時期ではないと判断された場合には、処理を終了する。一方、登録バイオ・データの更新時期であると判断された場合には、後処理部55はユーザ端末3から受信した入力バイオ・データを会員バイオ情報DB57に登録する（ステップS107）。これにて処理を終了する。なお、入力バイオ・データに対して処理を施した結果のデータを登録することもある。

【0046】一方、ステップS93において認証失敗と判断された場合には、バイオ認証処理部53は認証処理回数は許容限度内（例えば3回）であるか判断する（ステップS109）。もし、認証処理回数が許容限度内であれば、ステップS81に戻り、ユーザ端末3にバイオ・データの送信要求を送信する。一方、認証処理回数が許容限度を超えていれば、認証失敗をECサーバ7及びユーザ端末3に送信する（ステップS111）。もし、キーを用いた処理系の場合には、このときに隠しパラメータとしてECサーバ7に第2キーを送信する。

【0047】ECサーバ7は、バイオ認証サーバ5から認証失敗を受信すると（ステップS113）、認証要求を無効として取り扱う（ステップS115）。すなわち、発注受付を送信しないようにしたり、決済を実行したりせず、今回は受け付けられない旨の通知をユーザ端末3に行ったりする。また、ユーザ端末3は、認証失敗の情報を受信し（ステップS117）、処理を終了する。例えば、「今回認証できませんでした」といった表示を行う場合もある。

【0048】バイオ認証サーバ5のバイオ認証処理部53は、認証失敗を認証処理結果ログDB59に登録する（ステップS119）。

【0049】以上のような処理を実施することにより、バイオ認証サーバ5における認証処理も実施することができるようになり、従ってユーザによる不正行為等を防止することができるようになる。

【0050】以上本発明の一実施の形態を説明したが、本発明はこれに限定されるものではない。たとえば、ユーザ端末3にインストールされる認証処理プログラム33は、図1に示した以外の機能を有するような場合もあ

る。例えば、電子マネーを取り扱うための機能や、その他の決済の処理を安全に実施するための機能等である。バイオ認証サーバ5及び認証処理プログラム33の機能ブロックは、必ずしもプログラムのモジュールに対応しない。また、DBの管理の仕方や分け方についても図1に示したものは一例である。

【0051】さらに、図2乃至図5で説明した処理フローは一例であり、同様の処理を実施するためにステップの順番を入れ替えることも可能な部分もある。また、同時に実施することが可能なステップもある。

【0052】なお、上で述べたような処理をコンピュータに実施させるプログラムを作成することも可能であって、当該プログラムは、例えばフレキシブル・ディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。なお、ネットワークを介して配布される場合もある。また、処理途中のデータについては、コンピュータのメモリに一時保管される。

#### 【0053】

【発明の効果】以上本発明により、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を実施するための技術を提供することができる。

【0054】また、センタ・サーバにおいて必要な時に登録されたバイオメトリクス・データの更新を要求を行うことができるようにするための技術を提供することが

できる。

【0055】さらに、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を安全に実施するための技術を提供することができる。

#### 【図面の簡単な説明】

【図1】本発明の一実施の形態に係るシステム概要図である。

【図2】本発明の一実施の形態における処理フローを示す図である。

【図3】本発明の一実施の形態における処理フローを示す図である。

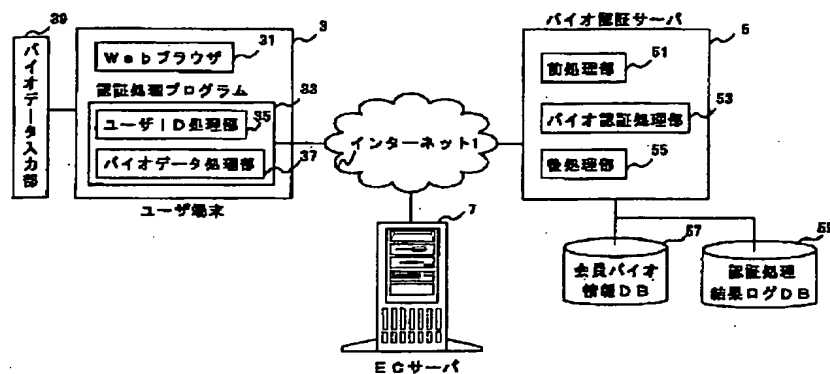
【図4】本発明の一実施の形態における処理フローを示す図である。

【図5】本発明の一実施の形態における処理フローを示す図である。

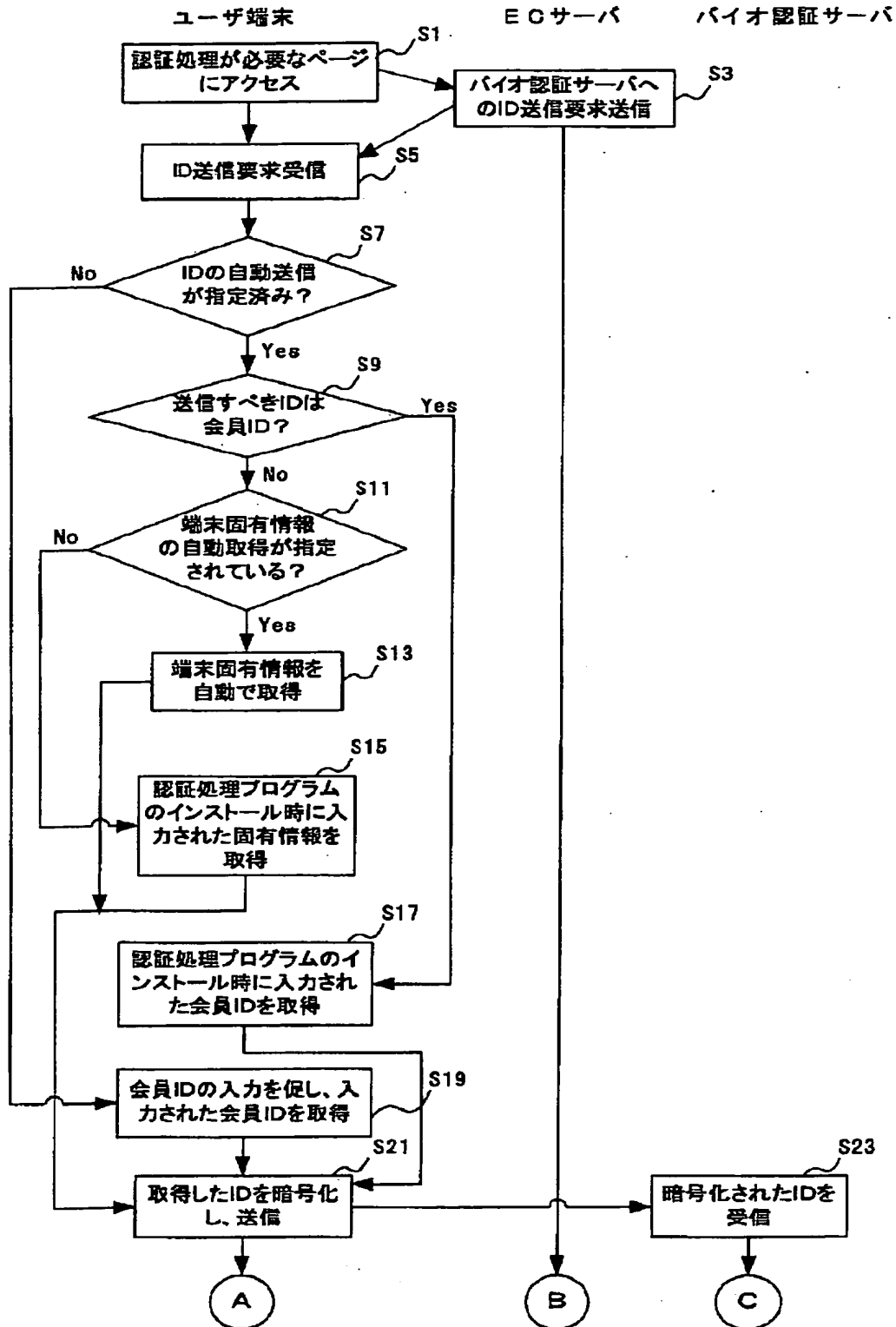
#### 【符号の説明】

1	インターネット	3	ユーザ端末	5	バイオ認証サーバ
7	ECサーバ	31	Webブラウザ	33	認証処理プログラム
35	ユーザID処理部	37	バイオデータ処理部	51	前処理部
39	バイオデータ入力部	53	バイオ認証処理部	55	後処理部
57	会員バイオ情報DB	59	認証処理結果ログDB		

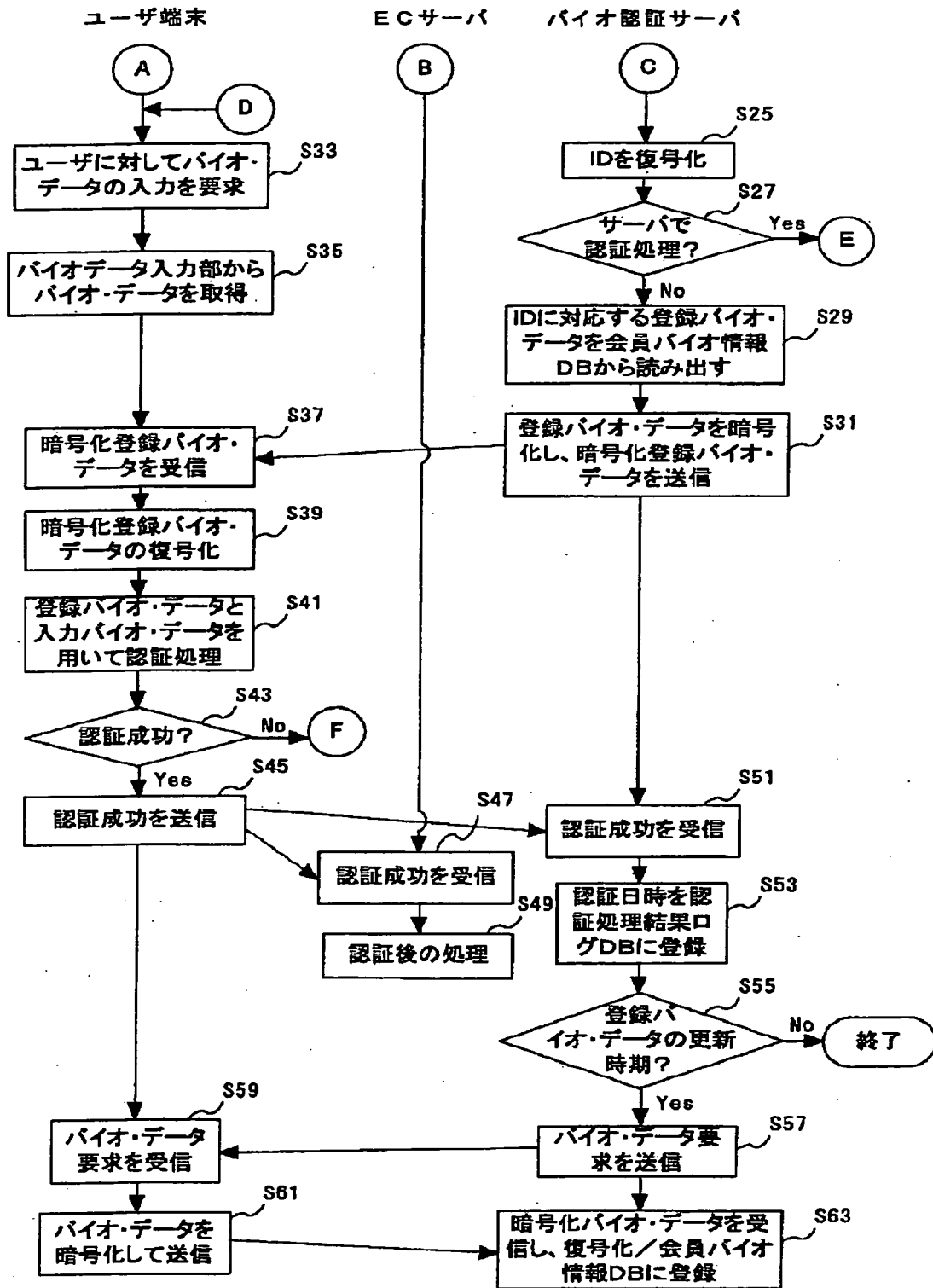
【図1】



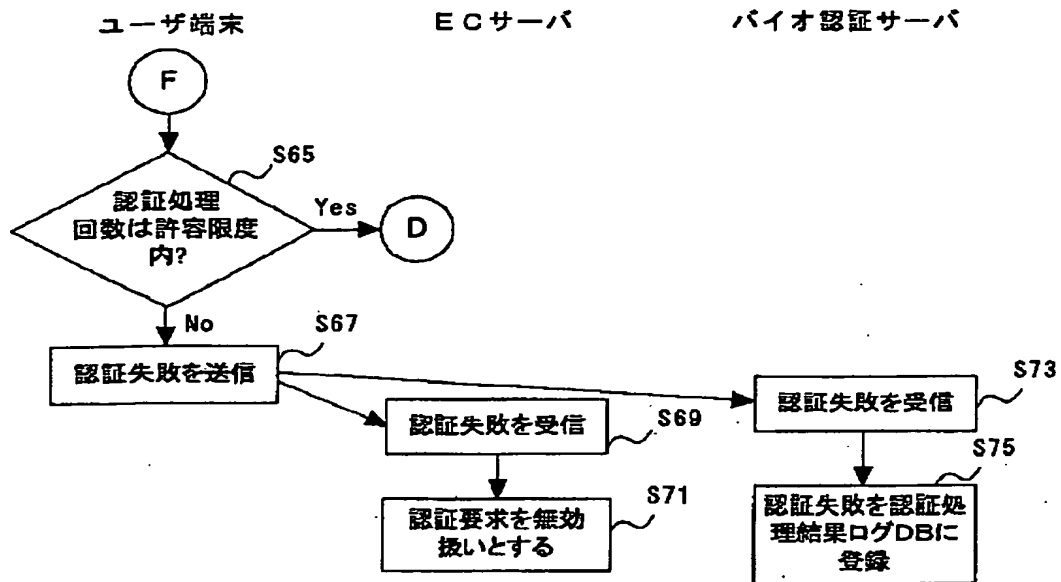
【図2】



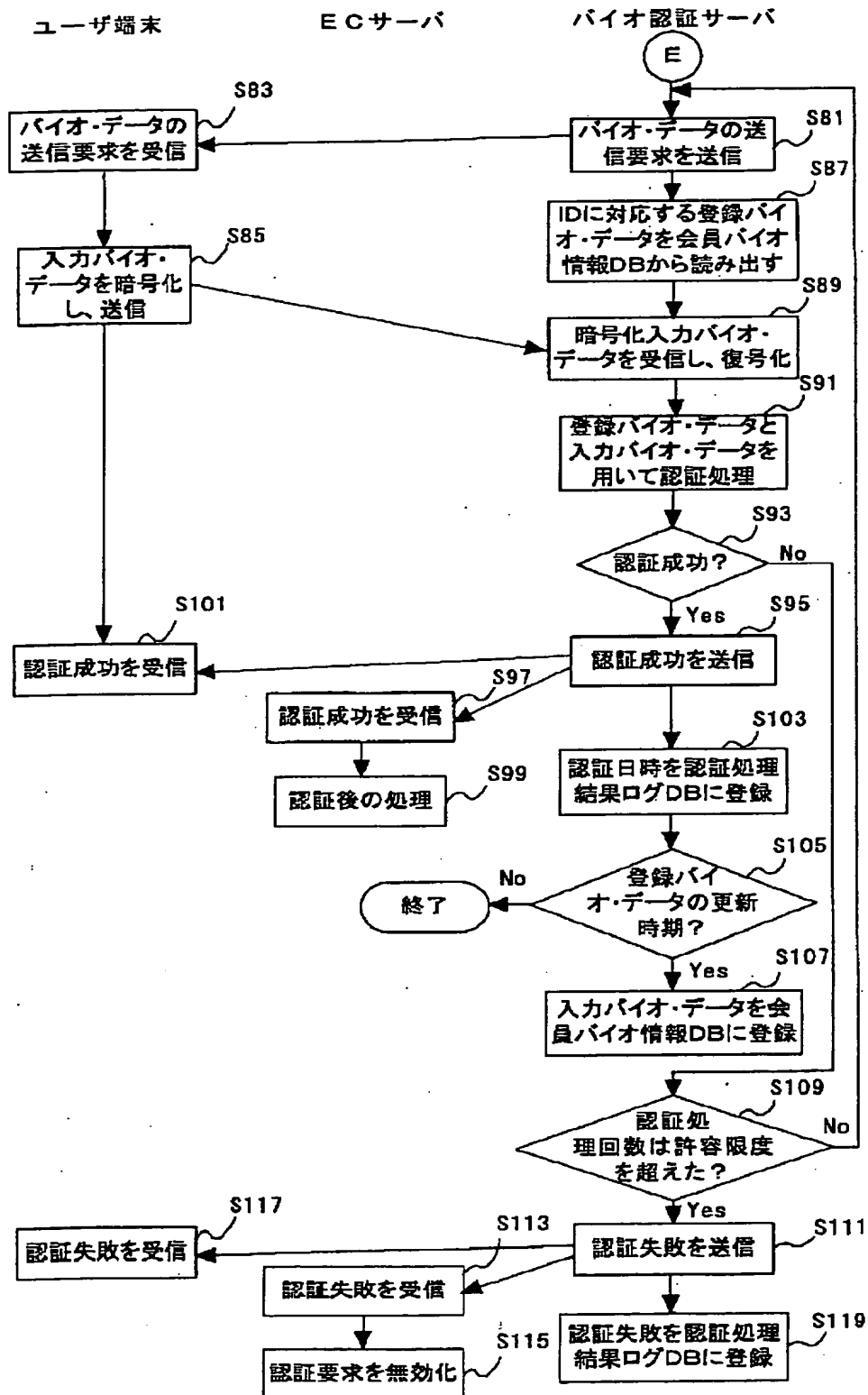
【図3】



【図4】



【図5】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**